

REMARKS

Please reconsider the application in view of the above amendments and the following remarks. Applicant thanks the Examiner for the courtesies extended in the telephonic Examiner interview of December 11, 2006, and for carefully considering this application.

Acknowledgement of Claim of Benefit

Applicant amended the Claim of Benefit in the "Amendments to the Specification" section, above. Applicant respectfully requests that the Examiner acknowledge this application's claim of benefit to provisional application 60/264,101 filed on January 25, 2001.

Disposition of the Claims

Claims 1-9, 13-25, and 28-35 were pending in the present application. Claims 1, 14, 15, 20, 21, 23, 24, 34, and 35 are independent. The remaining claims depend, directly or indirectly, from claim 1, 15, 21, or 24.

Request for Examiner Interview

Applicant respectfully requests an Examiner Interview to discuss the referenced application at a date and time convenient for all parties. An Applicant Initiated Interview Request Form is attached to this reply.

Claim Amendments

Independent claims 1, 14, 15, 20, 21, 23, 24, 34, and 35 have been amended by way of this reply. Specifically, these claims have been amended to specify that all communications from the dial-up client and from the server are transmitted via the remote access switch. No new matter has been added by way of these amendments, as support for these amendments may be found, for example, in Figure 3 of the Specification as published. Additionally, claims 1, 14, 21, 23, 24, 34, and 35 have been amended to specify that the server is connected to the remote access switch via a wide area network (*e.g.*, a wired connection), and claims 1, 14, 24, 34, 35 have been amended to specify that the dial-up client is configured to dial into the remote access switch (*i.e.*, the client computer established a dial-up connection with the remote access switch). No new matter has been added by way of these amendments, as support for these amendments may be found, for example, in Figure 3 and in paragraphs [0037]-[0038] of the Specification as published. Additionally, the independent claims have been amended to be in a more readable format and to correct minor typographical errors. No new matter has been added by way of these amendments. A clean copy of the claims as amended is attached for the Examiner's convenience.

Rejections under 35 U.S.C. § 103

Claims 1-9, 13-25, and 28-35 are rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,061,796 ("Chen") in view of U.S. Patent No. 6,772,341 ("Shrader") and in further view of U.S. Patent No. 6,377,691 ("Swift"). Independent claims 1, 14, 15, 20, 21, 23, 24, 34, and 35 have been amended as discussed above. To the extent this rejection applies to the amended claims, this rejection is respectfully traversed.

The claimed invention relates to a network system having a client computer and a server. A dial-up client executes on the client computer to dial a remote access switch, which serves as a link between the client computer and the server. The server is connected to the remote access switch via a wide-area network connection (e.g., a wired network). Using this configuration, all communication between the client computer, via a dial-up client loaded on the client computer, and the server is transmitted via the remote access switch (*see, e.g.*, Specification as published, Figure 3, paragraphs [0037]-[0038]).

The dial-up client loads and executes a custom script dynamically linked library, which is an interface to a client side cryptographic function on the client computer (*see, e.g.*, Specification as published, paragraphs [0039]-[0042]). The client-side cryptographic function provides a response to a challenge generated by the server in order to authenticate the user (*see, e.g.*, Specification as published, paragraph [0045]). The server also includes a PKI-bridge that is the interface between the server and a server side cryptographic function. After receiving and verifying the response to the generated challenge string, the server-side cryptographic function instructs the server to send a message to the remote access switch to allow or deny a connection between the client computer and the remote access switch. The instruction is sent from the server-side cryptographic function through the PKI-bridge to the server, and the server sends the message to the remote access switch via the wide-area network connection (*see, e.g.*, Specification as published, paragraphs [0053]-[0054]; [0057]-[0062]).

Turning to the rejection, to establish a *prima facie* case of obviousness "...the prior art reference (or references when combined) must teach or suggest all the claim limitations" (*see* MPEP § 2143.03). Further, "all words in a claim must be considered in judging the patentability of that

claim against the prior art" (*see, MPEP § 2143.03*). Applicant respectfully asserts that the cited references, when considered separately or in combination, fail to teach or suggest all the claim limitations of the amended claims. Specifically, the cited references fail to teach or suggest at least that: (i) all communications from the dial-up client and from the server are transmitted via the remote access switch, and (ii) the dial-up client is connected to the remote access switch via a dial-up connection and the server is connected to the remote access switch via a network connection, for at least the following reasons.

Chen does not teach or suggest a remote access switch

Chen does not teach or suggest a remote access switch as required by the claimed invention. Specifically, the claimed invention requires that the dial-up client is configured to dial into a remote access switch and that the server is configured to inform the remote access switch about whether to allow or deny a connection from the client computer. In contrast, in Chen, the only type of connection disclosed is performed through *an open network* (*see, e.g., Chen, col. 1 lines 26-36 and Figure 6*). In order to gain connection and authentication to a protected server at the end of an open network, a client must first be authenticated to an access point (*e.g., an Internet service provider*) within the open network. Only after being authenticated to the access point of the open network may the client then begin authentication with a protected server. Thus, Chen does not disclose an entity (*e.g., the remote access switch of the claimed invention*) that is dialed into by a client and that can be informed by the server performing the verification of the client whether to allow or deny the client's connection. Thus, Chen does not teach or suggest a remote access switch as required by the claimed invention.

Chen does not teach or suggest that the server is connected to the remote access switch via a wide-area network and that the dial-up client is configured to dial into the remote access switch.

Chen does not teach or suggest that the dial-up client is connected to the remote access switch via a dial-up connection and the server is connected to the remote access switch via a wide-area network connection. As discussed during the telephonic Examiner interview of December 11, 2006, Chen merely discusses Internet Protocol (IP) communication *directly* between a client computer and a server, over any network (*see* Chen, Figure 6, col. 8, lines 43-56, col. 10, lines 43-65). Thus, Chen does not teach or suggest at least that the dial-up client is connected to the remote access switch via a dial-up connection and the server is connected to the remote access switch via a network connection, as required by the claimed invention. Said another way, the claimed invention operates over a hybrid network (*i.e.*, a portion of the communication channel operates over a dial-up connection while another portion of the communication channel operates over a wide area network (*i.e.*, a wired connection)), while Chen operations over a homogeneous network (*i.e.*, the entire network is of the same type).

Chen does not teach or suggest that all communications from the dial-up client and from the server are transmitted via the remote access switch.

As discussed in the telephonic Examiner interview of December 11, 2006, Chen does not teach or suggest that all communications from the dial-up client and from the server are transmitted via the remote access switch. In contrast to the claimed invention, Chen teaches the use of a direct connection (communications links **60, 61**) between a SmartGATE client and a SmartGATE server,

and a direct link 62 for a peer-to-peer connection between two client applications. Accordingly, a request for authentication is made *directly* from one client computer to another client computer, or to a server. Thus, it would be clear to one skilled in the art that Chen does not teach or suggest at least that all communications from the dial-up client and from the server are transmitted via the remote access switch, as required by the claimed invention. Said another way, there is no device in Chen interposed between the client and the server through which *all* communication between the client and the server must pass.

Shrader and Swift do not teach that which Chen lacks

In view of the above, Chen fails to disclose all the limitations of amended independent claims. Further, Shrader and Swift do not teach that which Chen lacks. This is evidenced by the fact that Shrader is only relied upon to teach a directory server accessed by a server-side cryptographic function and that Swift is only relied upon to teach challenge string/response string encryption (see Office Action mailed September 21, 2006, at pages 5-6). Further, there is no discussion in either Shrader or Swift directed to the claimed connections between the client, the remote access switch, and the server, or to all communications between the dial-up client and the server being transmitted via the remote access switch, as recited in the amended claims.

In view of the above, Chen, Shrader, and Swift, whether considered separately or in combination, fail to support the rejection of amended independent claims 1, 14, 15, 20, 21, 23, 24, 34, and 35. Dependent claims 2-9, 13, 16-19, 22, 25, and 28-33, which depend directly or indirectly from the aforementioned independent claims, are allowable for at least the same reasons as the

aforementioned independent claims. Accordingly, withdrawal of this rejection is respectfully requested.

Further, the Applicant respectfully asserts that Chen, Shrader, and Swift fail to teach or suggest the limitations recited in claim 19 (*i.e.*, “wherein the dial-up client automates the authentication process using a hidden terminal operating in terminal mode”). In asserting that claim 19 is obvious, the Examiner has cited Figure 2, reference numeral 25 (*see* Office Action mailed September 21, 2006, p. 7). A review of Chen reveals that reference numeral 25 corresponds to a “modem connection” and that the remainder of Chen is completely silent with respect to using a hidden terminal as recited in claim 19. Further, Shrader and Swift are also completely silent with respect to a hidden terminal. In view of the above, claim 19 is patentable over the cited prior art for at least this additional reason. Accordingly, withdrawal of this rejection with respect to claim 19 is respectfully requested.

Conclusion

Applicant believes this reply is fully responsive to all outstanding issues and places this application in condition for allowance. If this belief is incorrect, or other issues arise, the Examiner is encouraged to contact the undersigned or his associates at the telephone number listed below. Please apply any charges not covered, or any credits, to Deposit Account 50-0591 (Reference Number 09469/006001).

Dated: December 21, 2006

Respectfully submitted,

By  #L031
Robert P. Lord
Registration No.: 46,479
OSHA · LIANG LLP
1221 McKinney St., Suite 2800
Houston, Texas 77010
(713) 228-8600
(713) 228-8778 (Fax)
Attorney for Applicant

Enclosures (Clean Copy of Amendments to the claims)
(Applicant Initiated Interview Request Form)